

REMARKS

I. Introduction

In the July 1, 2005, Office Action in this application, the United States Patent and Trademark Office (hereinafter "Office Action") rejected Claims 1, 3, 5-7, 9, 10, 12-19, 24-26, 30-37, and 41-45 under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 6,260,145, to Komura et al. (hereinafter "Komura"). Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 were rejected under 35 U.S.C. § 103(a) as unpatentable over Komura in view of U.S. Patent No. 6,715,073, to An et al. (hereinafter "An et al."). For the following reasons, applicant asserts that the claims of the present application are not anticipated or obvious over the cited and applied prior art, alone or in combination, because the prior art fails to teach or suggest a document processing server which encrypts and processes the document obtained from a sender, and provides the processed document to recipients through a secured communication channel as recited in the claims of the present invention. Prior to discussing more detailed reasons why applicant believes that the claims of the present application are allowable, a brief description of the present invention and the cited references are presented.

A. Summary of the Claimed Invention

In accordance with the present invention, a system and method for processing communications between a sender computing device and at least one recipient computing device are provided. Initially, a sender establishes a secure communication with a *document processing server* and requests the processing of an electronic document, which can include the appending of a digital signature. The document processing server processes the electronic document and establishes secure communications with one or more designated recipients. Further, upon sender's request, the document processing server implements sender-specified recipient identity verification and provides further processing of the electronic document as designated by the

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

recipients. In this manner, the sender and the designated recipient do not have to exchange any encryption keys, including a private encryption key, since the sender and the recipient communicate only with the document processing server, not each other. The document processing server is responsible for any processing relating to identification and encryption/decryption of the document.

B. Summary of Komura (U.S. Patent No. 6,260,145)

Komura discloses a system and method for authenticating digital information. Initially, a server appends verification data to an electronic document to be circulated through terminal units for persons in charge. Each terminal unit is allocated a unique function in advance. The server sends the document with verification data appended to the first terminal unit in a predetermined route (a route for circulation). *Each terminal unit sends the document directly to a next terminal unit* in the predetermined route and applies its unique function to the verification data in turn when receiving the document. The last terminal unit in the predetermined route sends the document with verification data back to the server. Upon receipt of the electronic document that has been circulated through the terminal units for persons in charge, the server examines the function-applied value appended to the document to determine whether the document has been circulated correctly through the persons in charge, or via the correct route. However, Komura fails to teach a server for establishing a secure communication with each terminal unit or being responsible for any processing relating to identification and encryption/decryption of the document.

C. Summary of An et al. (U.S. Patent No. 6,715,073)

An et al. discloses a system and method for *managing* the issuance, renewal, and revocation of *digital certificates* for Web browsers and servers using vault technology. Generally, the vault technology provides a secure environment in a web server using a vault

controller for running a secure Web-based registration process and enabling secure application. The controller provides security from other processes running on the same server and secure areas, or personal storage vaults to which only the owner has a key. System operators, administrators, certificate authorities, registration authorities, and others cannot get to stored information or secure processes in such personal vaults. The system in An et al. includes registration and certification authorities, and a Web server (vault controller) having personal storage vaults in the controller for users. Each personal vault runs programs on the controller under a unique UNIX user ID. This particular UNIX user ID is linked to a user with a specific vault access certificate. The content of the vault is encrypted and contains an encryption key pair and a signing key pair, both of which are password protected. Data storage provided by the controller, is owned by the same user ID assigned to the vault. A registration authority running as a software application in the controller processes requests to issue, renew and revoke *digital certificates* issued by a certification authority using *two pairs of public-private keys*.

II. Rejection of Claims 1, 3, 5-7, 9, 10, 12-19, 24-26, 30-37, and 41-45
Under 35 U.S.C. § 102

The Office Action rejected Claims 1, 3, 5-7, 9, 10, 12-19, 24-26, 30-37, and 41-45 under 35 U.S.C. § 102(b) as being anticipated by Komura. The Office Action asserts that Komura discloses each and every element of these claims. As described in more detail below, applicant respectfully disagrees.

A. Claim 1

Claim 1 recites:

A method for processing communications between a sender and at least one recipient, the method comprising:
obtaining a request from the sender to transmit an electronic document to at least one recipient;
obtaining an electronic document corresponding to the request from the sender;

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

processing the electronic document, wherein processing the electronic document includes encrypting the electronic document with an encryption key corresponding to the designated at least one recipient; establishing a communication channel with the designated at least one recipient; and

transmitting the processed electronic document to the designated at least one recipient;

wherein the sender and the designated at least one recipient do not exchange encryption keys.

Claim 1 recites a method for processing secured communications in a document processing server without requiring exchange of encryption keys between the sender and the recipient. The claimed method specifically recites "processing the electronic document, wherein processing the electronic document includes encrypting the electronic document with an encryption key corresponding to the designated at least one recipient and establishing a communication channel with the designated at least one recipient." Additionally, Claim 1 recites "transmitting the processed electronic document to the designated at least one recipient" such that "the sender and the designated at least one recipient do not exchange encryption keys."

Simply stated, the method disclosed in Komura does not establish a communication channel with designated recipients in order to transmit the processed electronic document which was obtained from a sender as recited in Claim 1. As the Office Action indicates, Komura merely discloses an interface (IF 21 in FIGURE 2) connecting a server and a first terminal unit in a predetermined route. See FIGURE 2 of Komura. However, the server in Komura does not establish a communication channel with each of the terminal units in the predetermined route. As mentioned above, the server sends the document with verification data appended to the first terminal unit in the predetermined route (circulation route). *Each terminal unit sends the document directly to a next terminal unit in the predetermined route and applies its unique function to the verification data in turn when receiving the document. The unique function is allocated to each terminal unit in advance. The last terminal unit in the predetermined route*

sends the document with verification data back to the server. Upon receipt of the electronic document that has been circulated through the terminal units for persons in charge, *the server examines the function-applied value appended to the document to determine whether the document has been circulated correctly through the persons in charge*, or via the correct route. For the reason set forth above, Komura fails to teach establishing a communication channel to each recipient upon receipt of the transmit request from the sender as recited in Claim 1.

Further, Komura fails to teach "the sender and the designated at least one recipient do not exchange encryption keys," as recited in Claim 1. However, the Office Action alleges that Komura inherently teaches such a limitation "by virtue of teaching the public key encryption system, which does not use exchange of encryption keys," relying on Col. 5, lines 15-20 of Komura. Office Action, p. 3, lines 8-11. The text from Komura discloses:

An example of a way for the data recipient to verify the originator's identity is to decrypt the digital signature using a public key described in a certificate published by an authentication office, and verify its contents. The secret key used to create the digital signature and the public key described in the certificate are paired with each other, so that data encrypted by using *the secret key can be decrypted by using the public key*.

The cited passage discloses that a secret key and a public key can be paired with each other to verify the originator's identity. One of ordinary skill in the art would understand that a public key in the public key encryption system serves the purpose of encrypting and decrypting a particular secret key that is *exchanged* between a sender and a recipient. Thus, the cited passage teaches an exchange of an encryption key (i.e., an encrypted secret key which is use to encrypt data) between a sender and a recipient. This is contrary to the above mentioned limitation recited in Claim 1. For the reasons set forth above, the cited passage fails to disclose "the sender and the designated at least one recipient do not exchange encryption keys," as recited in Claim 1.

To establish a proper rejection under 35 U.S.C. § 102, M.P.E.P. § 2131 states that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 further states that "[t]he identical invention must be shown in as complete detail as is contained in the. . . .claim." *Id.* Applicant respectfully submits that Komura fails to expressly or inherently teach, disclose, or suggest each and every element of Claim 1. Specifically, as explained above, Komura fails to disclose or suggest "processing the electronic document, wherein processing the electronic document includes encrypting the electronic document with an encryption key corresponding to the designated at least one recipient; establishing a communication channel with the designated at least one recipient," or "the sender and the designated at least one recipient do not exchange encryption keys." Accordingly, for this reason, applicant respectfully submits that the rejection of Claim 1 is in error and requests that it be withdrawn.

B. Claims 3, 5-7, 9, 10, and 12-18

Claims 3, 5-7, 9, 10, and 12-18 are dependent on Claim 1. For the above mentioned reasons with regard to Claim 1, applicant respectfully suggests that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the § 102 rejection with regard to dependent Claims 3, 5-7, 9, 10, and 12-18.

C. Claim 19

Claim 19 recites:

A system for processing communications, the system comprising:
a sender computing device operable to transmit a request to process an electronic document;
at least one recipient computing device corresponding to an identifiable communication channel; and
a document processing server, the document processing server operable to establish secure communications with the sender computing device and the at least one recipient computing device;

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

wherein the document processing server processes an electronic document and transmits the processed electronic document between the sender computing device and the recipient computing device without the sender computing device and the at least one recipient computing device exchanging encryption keys.

Applicant respectfully submits that Komura fails to teach or suggest each and every limitation recited in Claim 19. For example, Komura fails to teach "a document processing server" which is "operable to establish secure communications with the sender computing device and the at least one recipient computing device," as recited in Claim 19. However, the Office Action asserts that the above mentioned limitation "is met by server computing device in communication with document storage unit (31) and the recipients (12-14 in FIG. 2)". Office Action, p. 3, lines 14-17. Applicant respectfully disagrees.

Applicant submits that the server computing device (server) disclosed in Komura is patentably distinguishable over a document processing server as recited in Claim 19. While the document processing server in the claimed invention establishes a communication channel with each of the sender and the designated recipients so that the document processing server can receive a document from a sender and then transmit the document to each of the designated recipients, the server in Komura does not establish a communication channel with each of the designated recipients. Instead, the server in Komura sends the document with verification data appended only to a first terminal unit in a route. See Komura, Col. 6, lines 31-44. The first terminal unit then sends the document with its verification data to the next terminal unit, and so forth. See Komura, Col. 6, lines 45-67, Col. 7, lines 1-23. The way that the document is circulated in the predetermined route would lead one of ordinary skill in the art to believe that it is impossible for the server to send the document to each of the recipients via an established communication channel. Further, the server in Komura does not "processes an electronic document and transmits the processed electronic document between the sender computing device and the recipient computing device without the sender computing device and the at least one

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

recipient computing device exchanging encryption keys," as recited in Claim 19. In contrast, each terminal unit in Komura verifies the verification data upon receipt of the document, applies its unique function, appends a digital signature, and sends the document to a next terminal unit. In other words, in Komura, each terminal unit (not a server) processes a document and transmits the processed document to the next terminal unit in the predetermined route. For those reasons stated above, Komura fails to teach each and every limitation recited in Claim 19. Applicant respectfully requests withdrawal of the § 102 rejection with respect to Claim 19.

D. Claims 24-26, and 30-36

Claims 24-26, and 30-36 are dependent on Claim 19. As discussed above, Komura fails to teach or suggest each of the limitations recited in Claim 19. For the above mentioned reasons with regard to Claim 19, applicant respectfully asserts that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the § 102 rejection with regard to dependent Claims 24-26, and 30-36.

E. Claim 37

For similar reasoning with respect to Claims 1 and 19, applicant asserts that Komura does not teach "an interface component operable *to establish secure communication* with the sender computing device and the recipient computing device *without requiring the exchange of encryption keys* between the sender computing device and the recipient computing device," as recited in Claim 37. As described above, a server disclosed in Komura does not to establish secure communication with the sender computing device and the recipient computing device without requiring the exchange of encryption keys between the sender computing device and the recipient computing device. Accordingly, Komura fails to teach each and every limitation recited in Claim 37. Applicant respectfully requests withdrawal of the § 102 rejection with respect to Claim 37.

F. Claim 41-45

Claims 41-45 are dependent on Claim 37. As discussed above, Komura fails to teach or suggest each of the limitations recited in Claim 37. For the above mentioned reasons with regard to Claim 37, applicant respectfully asserts that the cited reference fails to teach each of the elements recited in the dependent claims. Accordingly, applicant respectfully requests withdrawal of the § 102 rejection with regard to dependent Claim 41-45.

III. Rejection of Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 Under 35 U.S.C. § 103

The Office Action rejected Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40 under 35 U.S.C. § 103(a) as being unpatentable over Komura in view of An et al. The Office Action asserts that Komura and An et al. suggest each and every element of these claims and that it would be obvious to combine the teachings of Komura and An et al. Applicant respectfully disagrees.

Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40

As described above, a primary reference, Komura, fails to teach, or suggest all the limitations of Claims 1, 19 and 37. The Office Action relies on An et al. for teaching a Web browser that is used to send a request for the client to the Web server, which the Office Action admits that Komura fails to disclose. However, An et al. does not make up the defects of Komura since An et al. merely teaches a system and method for *managing* the issuance, renewal, and revocation of *digital certificates* for Web browsers and servers using vault technology.

The system in An et al. includes a Web server (vault controller) having personal storage vaults in the controller for users, and registration and certification authorities. Each personal vault runs programs on the controller under a unique UNIX user ID. This particular UNIX user ID is linked to a user with a specific vault access certificate (*digital certificate*). The content of the vault is encrypted and contains an encryption key pair and a signing key pair, both of which

are password protected. A registration authority running as a software application in the controller processes requests to issue, renew, and revoke digital certificates issued by a certification authority using two pairs of public-private keys. In sum, An et al. is concerned about digital certificates to determine whether the Web browsers and servers should be authorized to access secure applications. However, the method disclosed in An et al. has nothing to do with "encrypting the electronic document with an encryption key corresponding to the designated at least one recipient and *establishing a communication channel* with the designated at least one recipient," as recited in Claim 1. Similarly, the system disclosed in An et al. has nothing to do with "a document processing server" or "an interface component" which is operable to *establish secure communications* with the sender computing device and the at least one recipient computing device without requiring the exchange of encryption keys between the sender computing device and the recipient computing device, as recited in Claims 19 and 37.

To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Ryoka*, 180 U.S.P.Q. 580 (C.C.P.A. 1974). *See also In re Wilson*, 165 U.S.P.Q. 494 (C.C.P.A. 1970).

Further, to establish a proper rejection under 35 U.S.C. § 103, M.P.E.P. § 2143 states that "three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations." (emphasis added) (MPEP § 2143). If an independent claim is nonobvious under 35 U.S.C. §103, then any claim depending therefrom is nonobvious. (emphasis added) *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

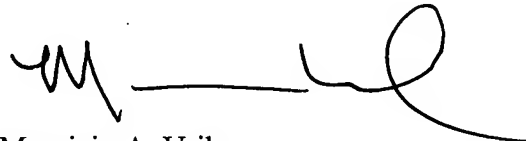
LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{PLLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100

As set forth above, the defects of Komura cannot be cured by An et al. Clearly, Komura and An et al., alone or much less in combination, fail to teach or suggest all the claim limitations recited in Claims 1, 19, and 37. Claims 2, 4, 8, and 11 depend from Claim 1. Claims 20-23, and 27-29 depend from Claim 19. Claims 38-40 depend from Claim 37. Applicant respectfully asserts that the cited references, alone or in combination, fail to teach all the claim limitations recited in the dependent claims. Accordingly, *prima facie* obviousness has not been established with respect to Claims 2, 4, 8, 11, 20-23, 27-29, and 38-40. Applicant respectfully requests withdrawal of all the pending § 103 rejections.

Conclusion

In view of the foregoing remarks, applicant submits that all pending claims are in patentable condition and respectfully requests an early notice to that effect. The Examiner is requested to contact applicant's attorney at the number provided below should any questions or issues remain.

Respectfully submitted,



Mauricio A. Uribe
Registration No. 46,206
Direct Dial No. 206.695.1728

I hereby certify that this correspondence is being deposited with the U.S. Postal Service in a sealed envelope as first class mail with postage thereon fully prepaid and addressed to Mail Stop AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the below date.

Date:

Jan. 3, 2006

Seri G. Hewes

SKL:lal

LAW OFFICES OF
CHRISTENSEN O'CONNOR JOHNSON KINDNESS^{LLC}
1420 Fifth Avenue
Suite 2800
Seattle, Washington 98101
206.682.8100